:UMENTATION PAGE

Form Approved
OMB No. 0704-0188

AD-A223 942

2. REPORT DATE: April 1990

3. REPORT TYPE AND DATES COVERED: Presentation/Paper

4. TITLE AND SUBTITLE: SAFENET OVERVIEW

5. FUNDING NUMBERS: PROJ: CC86
PE: SCN
WU: DN088539

6. AUTHOR(S): LT J. L. Paige, USN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES): Naval Ocean Systems Center
San Diego, CA 92152-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES): Naval Sea Systems Command
Washington, D.C. 20362

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT: Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The SAFENET program is an effort to develop network standards which support the needs of shipboard mission critical computer resources. There are currently two SAFENET standards in development, SAFENET I and SAFENET II. Each standard defines a communications subsystem which uses a local area network (LAN) to perform data transfer. Each standard is based on existing and proposed commercial network standards to reduce development time and cost, and to permit the use of commercial components whenever possible.

Published in *Proceedings of the Department of Defense Fiber Optics Conference '90*, March 1990.

14. SUBJECT TERMS: computer
display systems
data transmission

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS PAPER

SAFENET OVERVIEW

LT Jeffrey L. Paige, USN

Naval Ocean Systems Center, San Diego, CA

1. INTRODUCTION

The SAFENET program is an effort to develop network standards which support the needs of shipboard mission critical computer resources. There are currently two SAFENET standards in development, SAFENET I and SAFENET II. Each standard defines a communications subsystem which uses a local area network (LAN) to perform data transfer. Each standard is based on existing and proposed commercial network standards to reduce development time and [illegible], and to permit the use of commercial components whenever possible.

SAFENET I and II

The distinction between the two SAFENET standards is restricted to the commercial LAN standard which each is based upon. SAFENET I uses the IEEE 802.5 token-ring LAN which operates at 16 Mbps. In contrast, SAFENET II uses the emerging FDDI LAN which operates at 100 Mbps.

SAFENET Features

The SAFENET standards provide a system integrator with a number of significant features. First, each standard uses fiber optics for its transmission medium. Second, SAFENET contributes to system survivability by providing automatic fault isolation and reconfiguration. The standards also permit a variety of physical implementations, including embedded or stand-alone network interfaces. Finally, SAFENET is based on commercial standards, making it possible to obtain compliant networks and components from different vendors.

2. SAFENET PROFILE

SAFENET employs a layered protocol architecture which is based on the ISO/OSI reference model for computer networks. Within this layered architecture SAFENET specifies one or more protocols at each layer. The complete set of specified protocols is known as the SAFENET profile. The profiles for SAFENET I and II differ only in their LAN specifications.

The SAFENET communications architecture divides the protocol profile into three service partitions, each of which constitutes a portion of the seven layer ISO reference model. These SAFENET partitions are called user services, transfer services, and local area network (LAN) services. These partitions, the communication protocols they include, and their relationship to the ISO reference model are shown in Figure 1 for the SAFENET II profile.

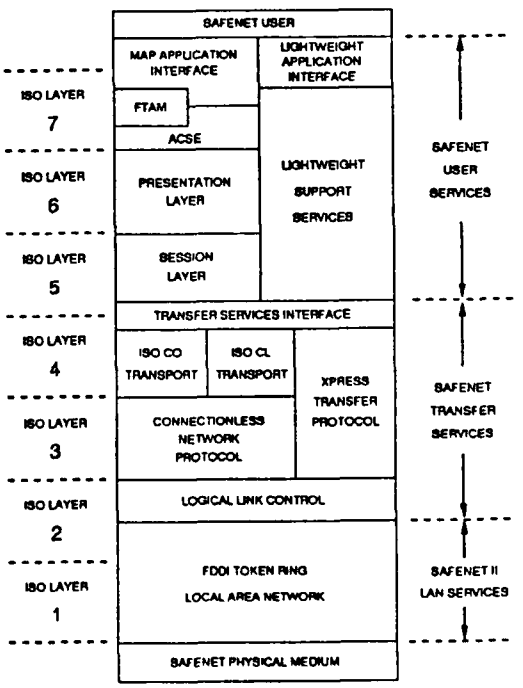

Figure 1. SAFENET II Protocol Profile

3. PROTOCOL SUITES

The SAFENET communications architecture can also be viewed in terms of its different protocol suites. In SAFENET, these are the OSI protocol suite, the lightweight protocol suite, and the combined protocol suite. These suites define the three distinct implementation classes permitted in SAFENET. In addition to these suites, each SAFENET profile includes some protocols and services which are common to all protocol suite implementations. These protocol suites, the communication protocols they include, and the communication protocols common to all suites are shown in Figure 2 for the SAFENET II profile. Note that the combined protocol suite is not shown as a distinct entity, since it is the union of the other two suites.

OSI Protocol Suite

The OSI protocol suite provides full OSI compliant networking to systems which require it. This suite's communication protocols are taken from the Manufacturing Automation Protocol (MAP) and the ISO connection-oriented transport protocol. The OSI protocol suite also includes the network management capabilities of MAP.

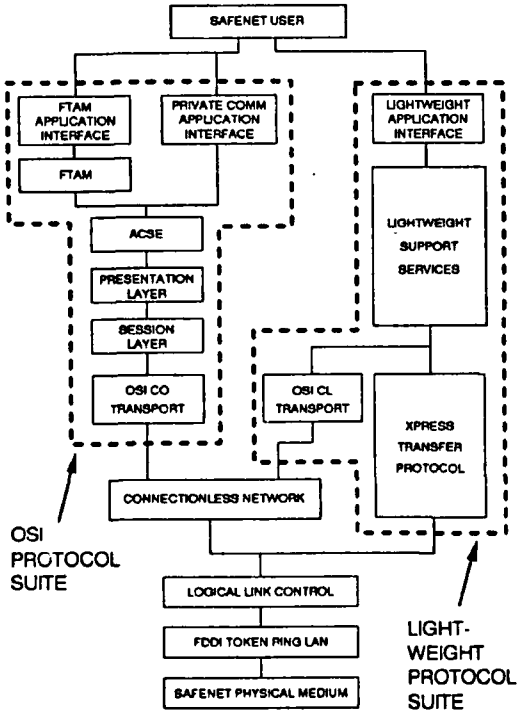

Figure 2. SAFENET II Protocol Suites

The OSI protocol suite is intended for situations where either the interoperability of independently developed SAFENET nodes is a driving consideration, or the file handling capabilities of FTAM is required, or the system is of such complexity that MAP network management is required. While the OSI protocol suite provides these capabilities, it does so at the expense of increased data transfer latency and an inability to send the same data to multiple users simultaneously (multicast).

Lightweight Protocol Suite

The lightweight protocol suite provides real-time data transfer to systems which require it. This suite's communication protocols are the Xpress Transfer Protocol (XTP) and the ISO connectionless transport protocol. The lightweight protocol suite also includes a SAFENET defined application interface. This suite has no defined network management capability.

The lightweight protocol suite is intended for situations where either data transfer latency is critical, or multicast data transfer is required, or system specific support services need to be implemented in place of ISO standard session, presentation, and application layer services. While the lightweight protocol suite provides these capabilities, it does so at the loss of the ISO standard protocols and network management mechanisms. Furthermore, since the lightweight protocol suite permits system specific implementation, interoperability is limited to those stations which have implemented identical lightweight suites.

Combined Protocol Suite

The combined protocol suite is essentially the union of the OSI and lightweight protocol suites. This suite therefore includes all the capabilities of those suites.

The combined protocol suite is intended for situations where the capabilities of both the OSI and lightweight protocol suites are required. The robust functionality of the combined protocol suite comes at the expense of the complexity of the system and the cost of its development

Services Common to all Suites

There are several features which are common to all SAFENET protocol suites. Foremost among these is the local area network specified for the particular

SAFENET standard (I or II) and the logical link control protocol. Because all stations on a given SAFENET share common protocols through the physical and data link layers, it is possible to attach stations which implement different protocol suites to the same LAN.

Another service common to any SAFENET network is the Global Time service. This service synchronizes time-of-day information around the network, and provides time values to application processes.

4. PHYSICAL TOPOLOGY

The SAFENET physical topology is shown in Figure 3 for SAFENET II. The SAFENET I topology differs from this only in the fact that single attachment stations are also permitted.

The key element in this topology is the trunk coupling unit (TCU). This is a device which enables a station to insert into or remove itself from a network ring. For SAFENET, the TCU is a 2x2 optical bypass switch. This switch is controlled an electrical signal from the attached station.

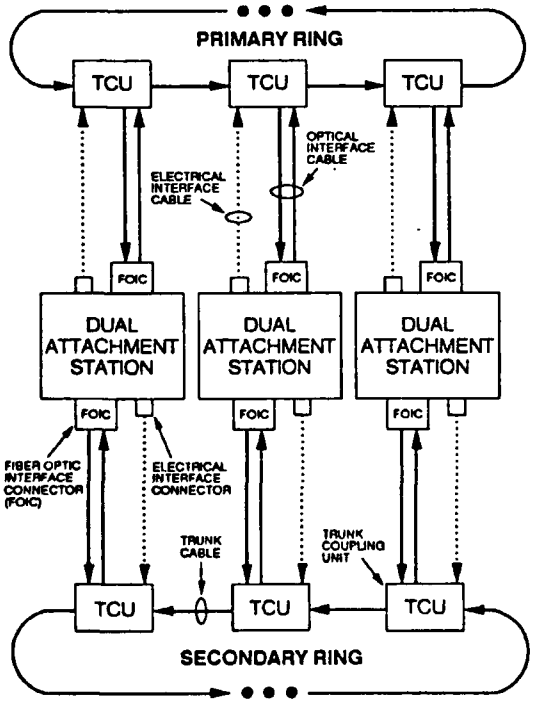

Figure 3. SAFENET II Physical Topology

Layout

Each network ring is comprised of a series of TCUs and connecting trunk cables. The primary and secondary ring trunk cables would be located apart from each other to avoid simultaneous damage to both rings. Each station attaches to a TCU via an optical interface cable and an electrical interface cable. A TCU and an attached station should be located apart from each other to optimize network survivablility.

Survivability

Each SAFENET standard is based on a dual counter-rotating ring LAN. This dual-ring architecture provides the capability for the network to automatically reconfigure in the presence of faults, such as a break in a trunk cable.

The SAFENET topology provides additional survivability by requiring each station to insert onto a ring by way of a trunk coupling unit (TCU). In the event of a station failure the TCU can be used to isolate the failed station from the ring, a procedure known as station bypass.

The SAFENET topology also provides survivability by permitting the key network components to be located apart from their attached stations, and the cables comprising the two network rings can by routed independently through the ship. These features allow the network to absorb some damage without losing its ability to operate.